



10/13/00

10/16/00

A

Please type a plus sign (+) inside this box → ☐PTO/SB/05 (12/97)
Approved for use through 09/30/00 ONB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

**UTILITY
PATENT APPLICATION
TRANSMITTAL**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney docket No. 00-1004

Total Pages 21

First Named Inventor or Application Identifier

Jonathan T. Huntington II

Express Mail Label No.

EF336478983US

10/13/00 U.S. PTO

09/687008

10/13/00

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification [Total Pages 10] 1
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross Reference to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure
3. ☒ Drawing(s) (35 USC 113) [Total Sheets 2] 1
4. Oath of Declaration [Total Pages 2] 1
a. ☐ Newly executed (original copy)
b. ☐ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting
inventor(s) named in the prior application,
see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a
copy of the oath of declaration is supplied under Box 4b,
is considered as being part of the disclosure of the
accompanying application and is hereby incorporated
by reference therein.

6. ☐ Microfiche Computer Program (Appendix)
7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement [] Power of Attorney
(when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure [] Copies of IDS
Statement (IDS)/PTO-1448 Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☐ Small Entity [] Statement filed in prior application,
Statement(s) Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☒ Other: Certificate of Express Mailing

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:

☐ Continuation ☐ Reissue ☐ Continuation-in-part (CIP) of prior application No _____**18. CORRESPONDENCE ADDRESS**☐ Customer Number or Bar Code Label

(Insert Customer No. or Attach bar code label here)

or ☒ Correspondence address below

NAME	Claudia Cameron				
ADDRESS	Phoenix Technologies Ltd. 411 East Plumeria Drive				
CITY	San Jose	STATE	CA	ZIP CODE	95134
COUNTRY	USA	TELEPHONE	(408) 570-1038	FAX	(408) 570-1044

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
FEE TRANSMITTAL LETTER

October 12, 2000

The Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the patent application, including four (4) sheet(s) of drawing,
of inventor(s): Jonathan T. Huntington II, et al.
for: Extensible Firmware Interface Virus Scan

Applicant is a small entity ☐; large entity ☒

The filing fee for this application is calculated below:

FOR:	CLAIMS AS FILED	RATE	TOTAL
Basic Fee		\$ 710.00 =	\$ 710.00
Total Claims	8 - 20 = 0 times	\$ 18.00 =	\$ 0.00
Independent Claims	1 - 3 = 0 times	\$ 80.00 =	\$ 0.00
Multiple Dependent Claims	0 times	\$ 270.00 =	\$ 0.00
TOTAL FILING FEE			\$ 710.00
Assignment Recording Fee	1 times	\$ 40.00 =	\$ 40.00
TOTAL FEES			\$ 750.00

A cheque in the amount of \$ **750.00** is enclosed with this Application Transmittal Letter to
cover the filing fees. This form is submitted in duplicate.

Respectfully submitted

Kenneth W. Float
Reg. No. 29,233

The Law Offices of Kenneth W. Float
Office address: 2 Shire, Coto de Caza, CA 92679
Mailing address: P. O. Box 80790, Rancho Santa Margarita, CA 92688
Telephone: (949) 459-5519
Facsimile: (949) 459-5520

PATENT
00-1004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Jonathan T. Huntington II, et al. : Date: October 12, 2000
Serial No. : Group Art Unit:
Filed: : Examiner:
For: Extensible Firmware Interface Virus Scan : Batch No.:

**CERTIFICATE OF MAILING
UNDER 37 CFR 1.10**

The Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Identification of Transmitted Papers

Utility Patent Application Transmittal form, patent application comprising nine (9) pages plus a cover page, two (2) sheets of drawing, Combined Declaration and Power of Attorney form, Assignment for recording, Recordation form cover sheet (PTO-1595), Fee Transmittal Letter in duplicate, cheque in the amount of \$750.00, and return receipt postcard

CERTIFICATION OF EXPRESS MAIL DEPOSIT

"EXPRESS MAIL" MAILING LABEL NO. EF336478983US

DATE OF DEPOSIT -October 13, 2000

I hereby certify that the above-identified correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service, under 37 CFR 1.10, on the date indicated above and addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.



Kenneth W. Float
Reg. No. 29,233

The Law Offices of Kenneth W. Float
Office Address: 2 Shire, Coto de Caza, CA 92679
Mailing Address: PO Box 80790, Rancho Santa Margarita, CA 92688
Telephone: (949) 459-5519
Facsimile: (949) 459-5520

PATENT
PD-00-1004

EXTENSIBLE FIRMWARE INTERFACE VIRUS SCAN

Jonathan T. Huntington II
Richard A. Bramley

[illegible][illegible][illegible][illegible][illegible][illegible]

The following US Patents were uncovered in a search of the US Patent and Trademark Office patent database records by the present inventors that address software virus protection: US Patent No. 5,764,889, issued June 9, 1998 entitled "Method and apparatus for creating a security environment for a user task in a client/server system";

5 US Patent No. 5,032,979, issued July 16, 1991 entitled "Distributed security auditing subsystem for an operating system"; US Patent No. 5,815,573, issued September 29, 1998 entitled "Cryptographic key recovery system"; US Patent No. 5,796,830, issued August 18, 1998 entitled "Interoperable cryptographic key recovery system"; US Patent

10 No. 5,590,266, issued December 31, 1999 entitled "Integrity mechanism for data transfer in a windowing system"; US Patent No. 4,918,653, issued April 17, 1990 entitled "Trusted path mechanism for an operating system"; and US Patent No. 6,026,374, issued April 17, 2000 entitled "System and method for generating trusted descriptions of information products". These patents address conventional mechanisms for providing virus protection.

15 A new Industry standard ROM based operating system has been developed which is known as EFI, or the Extensible Firmware Interface, that operates to replace DOS (Disk Operating System) functionality. As such, the EFI is controlled by the basic input and output system (BIOS) of the computer. The EFI is part of the BIOS within a flash nonvolatile RAM, and it is guaranteed to execute before any other

20 operating systems are loaded or disk access is allowed. Virus protection is not generally available for this ROM based operating system. The present invention addresses this need.

It is an objective of the present invention to provide for a virus protection method (software or firmware) for use with computer systems employing the Extensible

25 Firmware Interface.

SUMMARY OF THE INVENTION

To accomplish the above and other objectives, the present invention provides for a secure method (implemented as software or firmware) for implementing virus

30 protection on a computer system comprising an Extensible Firmware Interface and a basic input and output system (BIOS). The method is designed to protect and remedy potential viruses.

The computer system includes a central processing unit, a hard disk, and a nonvolatile random access memory, such as a read-only-memory or flash memory

35 device. The Extensible Firmware Interface is a ROM-based operating system (i.e., stored in the read-only-memory or a flash random access memory) that provides disk

operating system (DOS) functionality for the computer system, and is controlled by the BIOS.

The Extensible Firmware Interface is a read-only-memory (ROM) based operating system that operates to replace traditional disk operating system (DOS) functionality. The Extensible Firmware Interface is controlled by the basic input and output system and executes before any other operating systems are loaded or disk access is allowed.

The present method comprises the following steps. A command shell of the Extensible Firmware Interface is modified to include a command that operates to copy the boot sector of the hard disk to the nonvolatile random access memory. The modified Extensible Firmware Interface is stored in the nonvolatile random access memory. When the computer system is initialized (booted), a boot sector of the hard disk is copied to the nonvolatile random access memory. The boot sector of the hard disk is automatically read back from the nonvolatile random access memory on each boot, which bypasses the boot sector access of the hard disk during system initialization.

An extra field may be added to a BIOS SETUP routine, which is part of the BIOS, that allows a user to enable or disable reading the boot record from nonvolatile random access memory on boot. In implementing this aspect of the present method, the BIOS SETUP routine is run, and the user is prompted to enable or disable reading the boot record from nonvolatile random access memory on boot. The use of the BIOS SETUP routine allows a user to recover if he or she changes the boot disk or intentionally changes the boot disk's boot record to change the operating system or partition of the hard disk.

The method may also be modified to require entry of a security signature to prevent unauthorized updating of the stored boot sector. In implementing this aspect of the present invention, the command shell of the Extensible Firmware Interface is modified to include a command a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface the security signature input field is displayed to a user. The required signature is then input by the user prior to updating the stored boot sector.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features and advantages of the present invention may be more readily understood with reference to the following detailed description taken in conjunction with the accompanying drawing, wherein like reference numerals designate like structural elements, and in which:

Fig. 1 illustrates a first embodiment of an exemplary computer system in which the present invention is employed;

Fig. 1a illustrates a second embodiment of an exemplary computer system in which the present invention is employed; and

5 Fig. 2 is a flow diagram that illustrates an exemplary method in accordance with the principles of the present invention for providing virus protection of a computer system.

DETAILED DESCRIPTION

10 Referring to the drawing figures, Fig. 1 illustrates a first embodiment of an exemplary computer system 10 in which the present invention is employed. The first embodiment represents a typical older computer system 10 constructed in accordance with the current state of the art.

The computer system 10 comprises a central processing unit (CPU) 11, which is
15 coupled to a hard disk 12, a read-only-memory (ROM) 13, and a nonvolatile random access memory (NVRAM) 14, also known as flash memory 14. The computer system 10 also comprises an Extensible Firmware Interface (EFI) 15 which is a ROM-based operating system (i.e., stored in the read-only-memory 13) that provides disk operating system (DOS) functionality for the computer system 10, along with a basic input and
20 output system (BIOS) 16.

In general, ROM and flash devices are considered by BIOS engineers to be substantially the same. Historically, the BIOS was located in ROM but, in modern computer systems, the BIOS and EFI are contained in flash devices, so there is no need for the distinction between ROM and NVRAM (flash) devices. It is to be understood
25 that the present invention does not exclude ROM devices, although substantially all currently produced personal computers are implemented using flash devices. A more current embodiment of the computer system 10 is discussed with reference to Fig. 1a.

The Extensible Firmware Interface 15 comprises a command shell, which is the outermost layer or user interface of this program, and which comprises a command
30 processor interface. The command processor is a program that executes operating system commands. The command shell is that part of the command processor that accepts commands. After verifying that the commands are valid, the shell sends them to another part of the command processor to be executed.

The basic input and output system 16, or BIOS 16, is a firmware program that is
35 stored in the nonvolatile random access memory 14 (or flash memory 14). The BIOS 16 brings up the computer system 10 when it is turned on. The Extensible Firmware

Interface 15 is controlled by the BIOS 16 and executes before any other operating systems are loaded or access is allowed to the hard disk 12.

The BIOS 16 determines what the computer can do without accessing programs from the hard disk 12 or other media. The BIOS 16 contains code required to control the keyboard, display screen, disk drives, serial communications, for example, along
 5 certain other functions, depending upon the computer system 10.

Fig. 1a illustrates a second embodiment of an exemplary computer system 10 in which the present invention is employed. The second embodiment represents a computer system 10 constructed in accordance with the current state of the art.

10 The second embodiment of the computer system 10 comprises a central processing unit (CPU) 11, which is coupled to a hard disk 12, and a nonvolatile random access memory (NVRAM) 14, or flash memory 14. The computer system 10 also comprises an Extensible Firmware Interface (EFI) 15 and a basic input and output system (BIOS) 16 stored in the NVRAM 14. The Extensible Firmware Interface 15
 15 and BIOS 16 function as discussed with reference to Fig. 1.

Fig. 2 is a flow diagram that illustrates an exemplary method 20 in accordance with the principles of the present invention for providing virus protection for the computer system 10. The method 20 is designed to protect and remedy potential viruses that are loaded onto the computer system 10.

20 The method 20 comprises software 20, and preferably firmware 20, that is used in conjunction with a computer system 10 comprising a central processing unit (CPU) 11, a hard disk 12, a nonvolatile memory (NVRAM) 14, a basic input and output system (BIOS) 16, and an Extensible Firmware Interface 15. The software 20 or firmware 20 stored and executed from the nonvolatile memory (NVRAM) 14 or ROM 13) of the
 25 computer system 10. The method 20 comprises the following steps.

A command shell of the Extensible Firmware Interface 15 is modified 21 to include a command, referred to as <saveboot>, that operates to copy the boot sector of the hard disk 12 to the nonvolatile random access memory 14. The modified Extensible
 Firmware Interface 15 is stored 22 in the nonvolatile random access memory 14.

30 When the computer system 10 is initialized (booted), a boot sector of the hard disk 12 is copied 23 to the nonvolatile random access memory 14. The boot sector of the hard disk 12 is automatically read back 24 from the nonvolatile random access memory 14 on each boot, which bypasses the boot sector access of the hard disk 12 during system initialization.

35 An extra field may be added 25 to a BIOS SETUP routine 17, which is part of the BIOS 16, that allows a user to enable or disable reading the boot record from nonvolatile random access memory 14 on boot. In implementing this aspect of the

present method 20, the BIOS SETUP portion of the BIOS is run 26, and the user is prompted to enable 27 or disable 28 reading the boot record from nonvolatile random access memory 14 on boot. The use of the BIOS SETUP routine 17 allows a user to recover if he or she changes the boot disk or intentionally changes the boot disk's boot record to change the operating system or partition of the hard disk 12.

The software 20 or firmware 20 that implements the method 20 may also be modified to require entry of a security signature to prevent unauthorized updating of the stored boot sector. In implementing this aspect of the present invention, the command shell of the Extensible Firmware Interface 15 is further modified 31 to include a command a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface 15 the security signature input field is displayed 32 to a user. The required signature is then input 33 by the user prior to updating the stored boot sector.

The method 20 is fast because the operating system does not need to scan the boot sector for a long list of potential viruses during power on self test (POST). The method 20 is simple because it does not require any additional virus software. In addition to boot sector protection, additional software may be provided during the power on self test to scan for infection signatures in the nonvolatile random access memory 14 on each boot. Signature files may be provided in firmware or the nonvolatile random access memory 14 or from the hard disk 11. Remediation code may also be provided to remove infected boot sectors and viruses found in memory during power on self test. The present virus protection method may also replace or complement other virus protection programs.

Thus, a method that provides protection from software viruses on computer systems that use an extensible firmware interface has been disclosed. It is to be understood that the above-described embodiments are merely illustrative of some of the many specific embodiments that represent applications of the principles of the present invention. Clearly, numerous and other arrangements can be readily devised by those skilled in the art without departing from the scope of the invention.

CLAIMS

What is claimed is:

1. A method for providing virus protection of computer system comprising a central processing unit, a hard disk, a nonvolatile random access memory, an Extensible Firmware Interface, and a basic input and output system, the method comprising the steps of:

- 5 modifying a command shell of the Extensible Firmware Interface to include a command that operates to copy the boot sector of the hard disk to the nonvolatile random access memory;
- storing the modified Extensible Firmware Interface in the nonvolatile random access memory;
- 10 when the computer system is initialized, copying a boot sector of the hard disk to the nonvolatile random access memory;
- reading back the boot sector of the hard disk from the nonvolatile random access memory on each boot to bypass boot sector access of the hard disk during system initialization.

2. The method recited in Claim 1 which comprises software.

3. The method recited in Claim 1 which comprises firmware.

4. The method recited in Claim 1 further comprising the step of:
adding a field to a BIOS SETUP portion of the BIOS, that allows a user to enable or disable reading the boot record from nonvolatile random access memory on boot;

- 5 running the BIOS SETUP portion of the BIOS; and
- enabling or disabling reading the boot record from nonvolatile random access memory on boot.

5. The method recited in Claim 1 further comprising the step of:
further modifying the command shell of the Extensible Firmware Interface to include a command a security signature input field;

- 5 during execution of the Extensible Firmware Interface, displaying the security signature input field to a user; and
- inputting the required signature prior to updating the stored boot sector.

further modifying the command shell of the Extensible Firmware Interface to include a command a security signature input field;

during execution of the Extensible Firmware Interface, displaying the security

7. The method recited in Claim 1 wherein the modified Extensible Firmware

8. The method recited in Claim 1 wherein the modified Extensible Firmware

EXTENSIBLE FIRMWARE INTERFACE VIRUS SCAN

ABSTRACT

A secure method for implementing virus protection on a computer system having an Extensible Firmware Interface (EFI) and a basic input and output system (BIOS). The computer system has a hard disk, and a nonvolatile random access memory (NVRAM), such as a read-only-memory or flash device. To implement the functionality provided by the present invention, a command is added to the command shell of the Extensible Firmware Interface and stored in the NVRAM. This command automatically copies the boot sector of the hard disk to the NVRAM when the computer system is initialized. The boot sector of the hard disk is automatically read back from the NVRAM on each boot, which bypasses the boot sector access of the hard disk during system initialization, thus protecting and eliminating potential viruses. An field may be added to a BIOS SETUP routine that allows a user to enable or disable reading the boot record from NVRAM on boot. In implementing this, the BIOS SETUP routing is run, and the user is prompted to enable or disable reading the boot record from NVRAM on boot. The command shell of the EFI may also be modified to include a command to include a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface the security signature input field is displayed to a user. The required signature is then input by the user prior to updating the stored boot sector.

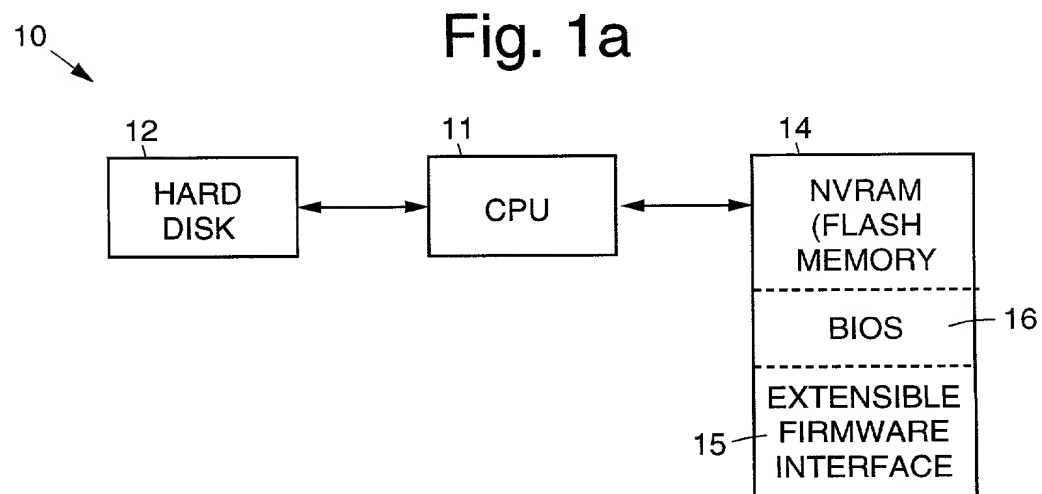
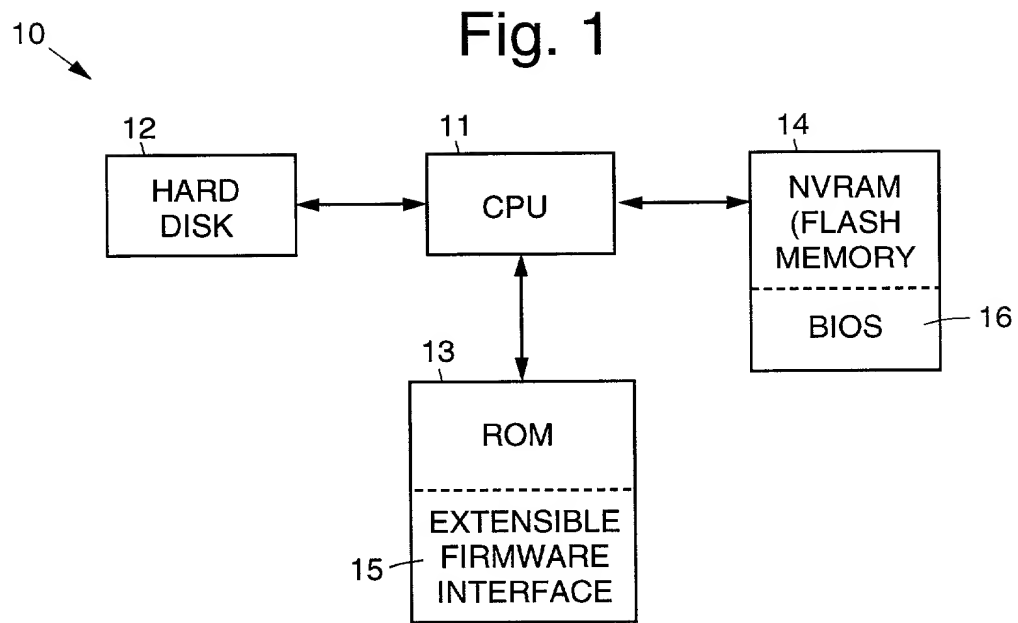
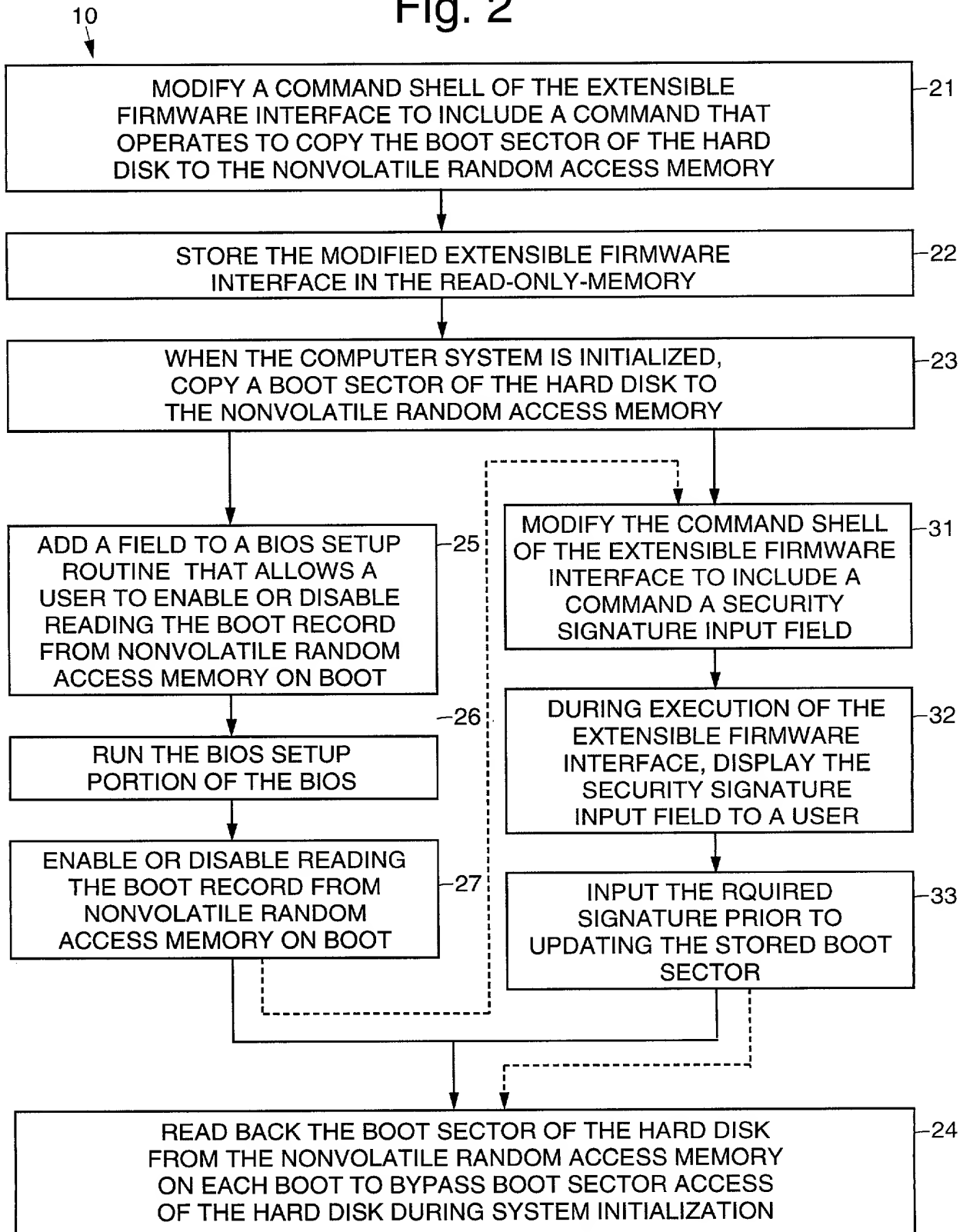


Fig. 2



**COMBINED DECLARATION FOR PATENT APPLICATION
AND POWER OF ATTORNEY**

Page 1 of 2
PD- 00-1004

- ☒ Original
☐ Continuation
☐ Division
☐ Continuation-in-part
☐ Supplemental
☐ PCT
☐ Design

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **Extensible Firmware Interface Virus Scan**

the specification of which

(check one) ☒ is attached hereto
☐ was filed on _____ as _____
Application Serial No. _____ and (a) [other than supplemental] was amended
on or (b) [supplemental] with amendments through _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of the application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority Claimed

_____ Number	_____ Country	_____ Day/Month/Year filed	<input type="checkbox"/> Yes <input type="checkbox"/> No
-----------------	------------------	-------------------------------	---

I hereby claim the benefit under Title 35, United States Code, §120 of any United States applications(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ Application Serial No.	_____ Filing Date	_____ Status (patented, pending, abandoned)
---------------------------------	----------------------	---

DECLARATION

Page 2 of 2

PD-00-1004

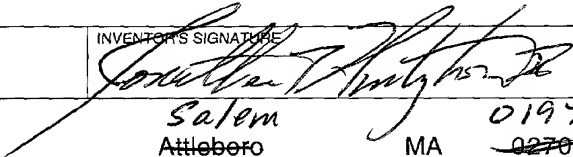
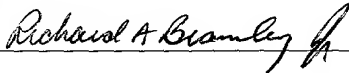
I hereby appoint the following attorneys, or agent and attorneys, to prosecute the application and to transact all business in the Patent and Trademark Office in connected therewith:

Kenneth W. Float, Registration No. 29,233

Address all correspondence to Claudia Cameron, Legal Assistant, Phoenix Technologies Ltd., 411 East Plumeria Drive, San Jose, CA 95134. Please address telephone calls to Claudia Cameron at (408) 570-1038

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false

United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST JOINT INVENTOR Jonathan T. Huntington II	INVENTOR'S SIGNATURE 	DATE 10/10/00
RESIDENCE 11 Winter Street	Salem Attleboro MA 01970 02703	CITIZENSHIP U.S.A.
POST OFFICE ADDRESS 11 Winter Street Salem MA 01970 157 Dexter Street, Attleboro, MA 02703		
FULL NAME OF JOINT INVENTOR Richard A. Bramley, Jr.	INVENTOR'S SIGNATURE 	DATE
RESIDENCE 12 Gloria Drive	Mansfield MA 02048	CITIZENSHIP U.S.A.
POST OFFICE ADDRESS 12 Gloria Drive, Mansfield, MA 02048		
FULL NAME OF JOINT INVENTOR	INVENTOR'S SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF JOINT INVENTOR	INVENTOR'S SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF JOINT INVENTOR	INVENTOR'S SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		
FULL NAME OF JOINT INVENTOR	INVENTOR'S SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		